ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ
INFORMATION TECHNOLOGIES AND TELECOMMUNICATION

УДК 004.75 **DOI: 10.18413/2518-1092-2019-4-3-0-7**

Кузнецов Д.А.[1]
Дамм В.А.[1]
Кузнецов А.В.[1]
Басов О.О.[2]

ПРИМЕНЕНИЕ МНОГОМОДАЛЬНОЙ АУТЕНТИФИКАЦИИ НА ОБЪЕКТАХ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

[1)] Федеральное государственное казённое военное образовательное учреждение высшего образования «Академия Федеральной службы охраны Российской Федерации», ул. Приборостроительная, д. 35, г. Орёл, 302034, Россия
[2)] Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», Кронверкский пр., д. 49, г. Санкт-Петербург, 197101, Россия

e-mail: wvxp@mail.ru, kvaa77@mail.ru, oobasov@mail.ru

Аннотация
Безопасность функционирования объектов критической информационной инфраструктуры Российской Федерации определяет высокий уровень обороноспособности государства, безопасности и правопорядка. В настоящее время применяемые на таких объектах традиционные системы аутентификации, подразумевающие использование факторов знания и владения в процессе предоставления прав доступа пользователям, в полной мере не отвечают предъявляемым требованиям. Такие системы обладают серьезными недостатками, обуславливающими их высокую уязвимость для злоумышленника. Использование биометрических методов одномодальной аутентификации также не лишено недостатков и не гарантирует высокий уровень безопасности автоматизированных систем. Проведенный анализ показал, что переход к системам многомодальной аутентификации позволяет выполнить требования, предъявляемым к системам аутентификации, а также существенно повысить уровень достоверности принятия решений и снизить вероятность возникновения ошибок.
Ключевые слова: интеллектуальное пространство; многомодальность; обнаружение лица; аутентификация; автоматизация; распознавание; контроль доступа.

UDC 004.75

Kuznetsov D.A.[1]
Damm V.A.[1]
Kuznetsov A.V.[1]
Basov O.O.[2]

APPLICATION OF MULTIMODAL AUTHENTICATION AT CRITICAL INFORMATION INFRASTRUCTURE FACILITIES

[1)] Federal state military educational institution of higher professional education "Academy of the Federal security service of the Russian Federation", 35 Priborostroitelnaya St, Orel, 302034, Russia
[2)] Saint Petersburg National Research University of Information Technologies, Mechanics and Optics, 49 Kronverkskiy prospekt, St. Petersburg, 197101, Russia

e-mail: wvxp@mail.ru, kvaa77@mail.ru, oobasov@mail.ru

Annotation
The security of the operation of the objects of the critical information infrastructure of the Russian Federation determines the high level of defense capacity of the State, security and law and order. At present, the traditional authentication systems used at such sites, which involve the use of knowledge and ownership factors in the process of granting access rights to users, do not fully meet the requirements. Such systems have serious disadvantages that make them highly vulnerable to the attacker. The use of biometric single-mode authentication methods is also not devoid of

disadvantages and does not guarantee a high level of security of automated systems. The analysis showed that the transition to multimodal authentication systems allows to meet the requirements of authentication systems, as well as to significantly increase the level of reliability of decision-making and reduce the probability of errors.
Keywords: intellectual space; multimodality; detection of the person; authentication; automation; recognition; access control.

ВВЕДЕНИЕ

Надежность и безопасность функционирования объектов критической информационной инфраструктуры (КИИ) Российской Федерации определяет высокий уровень обороноспособности государства, безопасности и правопорядка [1]. Важнейшим этапом обеспечения безопасности на таких объектах является аутентификация пользователей [2] информационных систем и автоматизированных систем управления [3] субъектов КИИ. Аутентификация пользователей на объектах КИИ, как правило, заключается в применении методов, направленных на разграничение доступа пользователей [4, 5]. Такие методы позволяют осуществить, в лучшем случае, двухфакторную аутентификацию с использованием электронного ключа и пароля, что в полной мере не снимает угрозу несанкционированного доступа к объектам и автоматизированным системам.

Анализ способов аутентификации пользователя в современных автоматизированных системах показал возможность отчуждения персонального идентификатора от пользователя, обуславливающую высокую уязвимость аутентификации. При любой сложности исполнения электронных устройств, предназначенных для аутентификации пользователя по фактору владения, существует возможность их подделки или утраты, что создает прецедент для получения доступа нелегитимным пользователем. Методы парольной аутентификации также обладают вышеназванными недостатками. Биометрическая аутентификации обладает рядом недостатков, вызванных возможностью предъявить такой системе фото, видео и голос легитимного пользователя, а также снижением достоверности при изменении физиологического состояния человека.

Наличие указанных недостатков диктует необходимость поиска решения, направленного на их устранение и выполнение требований безопасности, предъявляемых к объектам КИИ [2, 7].

ОСНОВНАЯ ЧАСТЬ

Критерии оценки систем аутентификации

Система аутентификации должна обладать следующими свойствами:

достоверность – способность устанавливать истинность пользователя с требуемой точностью;

непрерывность – способность обеспечивать процедуру аутентификации на протяжении всего времени работы пользователя;

защищенность – невозможность использования аутентификаторов другими лицами;

оперативность – способность проведения однократной аутентификации за установленное время;

ресурсоемкость – степень соответствия объема ресурсов системы аутентификации требуемому значению;

удобство использования – способность обеспечить комфортное пользование системой аутентификации.

К каждому свойству предъявляется ряд требований [3,10] (рис.1).

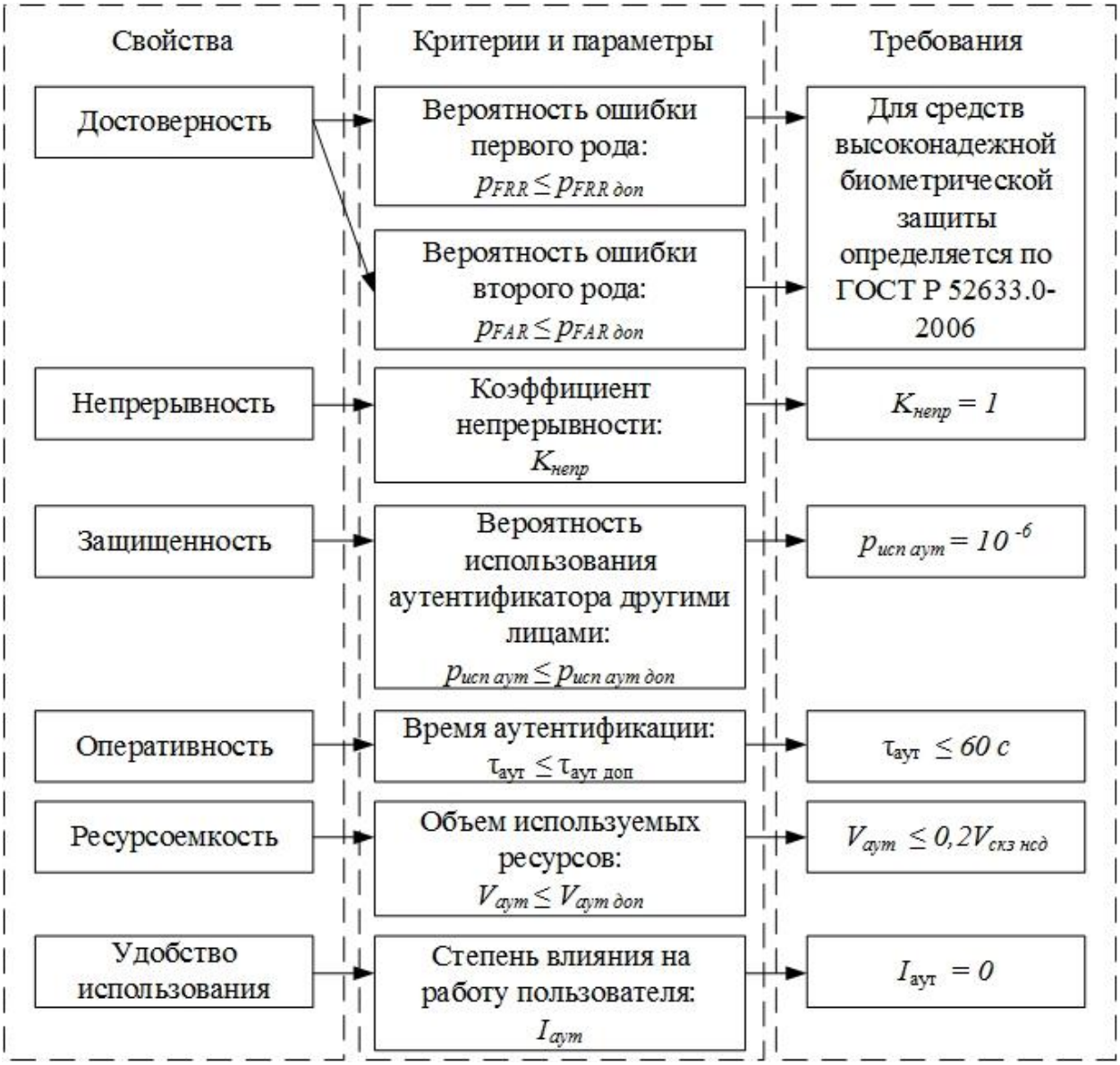

Рис. 1. Критерии и требования, предъявляемые к системе аутентификации
Fig. 1. The criteria and requirements for the authentication system

Очевидно, что основным является требование по достоверности аутентификации. Оно характеризуется вероятностью ошибок первого рода, т.е. вероятностью ошибочного отказа доступа легитимному пользователю, и вероятностью ошибок второго рода – вероятностью ошибочного предоставления доступа нелегитимному пользователю. При этом требования по вероятности ошибок первого рода предъявляются, в основном, к биометрическим системам аутентификации, так как в других случаях из-за особенностей функционирования систем такие ошибки практически отсутствуют. Поэтому анализ существующих систем аутентификации проведем исходя из их способности обеспечить требуемый уровень достоверности.

Анализ существующих систем аутентификации пользователя

В большинстве технических и программных средствах аутентификации, применяемых на объектах КИИ, используется сочетание классических методов аутентификации по фактору знания (пароль) и по фактору владения (персональный идентификатор) [4, 5, 8].

Надежность паролей основывается на способности человека помнить и хранить их в тайне, что обуславливает его простоту, однако такой пароль легко подобрать, получить с использованием

специального программного обеспечения, или подсмотреть (перехватить) с помощью технических средств.

Использование персональных идентификаторов подвержено угрозам их утраты и подделки, не смотря на применение различных методов их усложнения.

Преимущества биометрической аутентификации заключаются в невозможности использования уникальных индивидуальных признаков пользователя другими лицами, а изготовление поддельных биоматериалов связано с большими затратами, однако технически возможно, а в условиях девиации биометрических параметров пользователя произойдет снижение достоверности аутентификации.

Указанные недостатки обуславливают наличие ряда угроз (рис. 2), которым подвержены используемые в настоящее время факторы аутентификации, что не позволяет в полной мере обеспечить требуемый уровень достоверности процедуры аутентификации и, соответственно, предотвратить НСД к объектам КИИ.

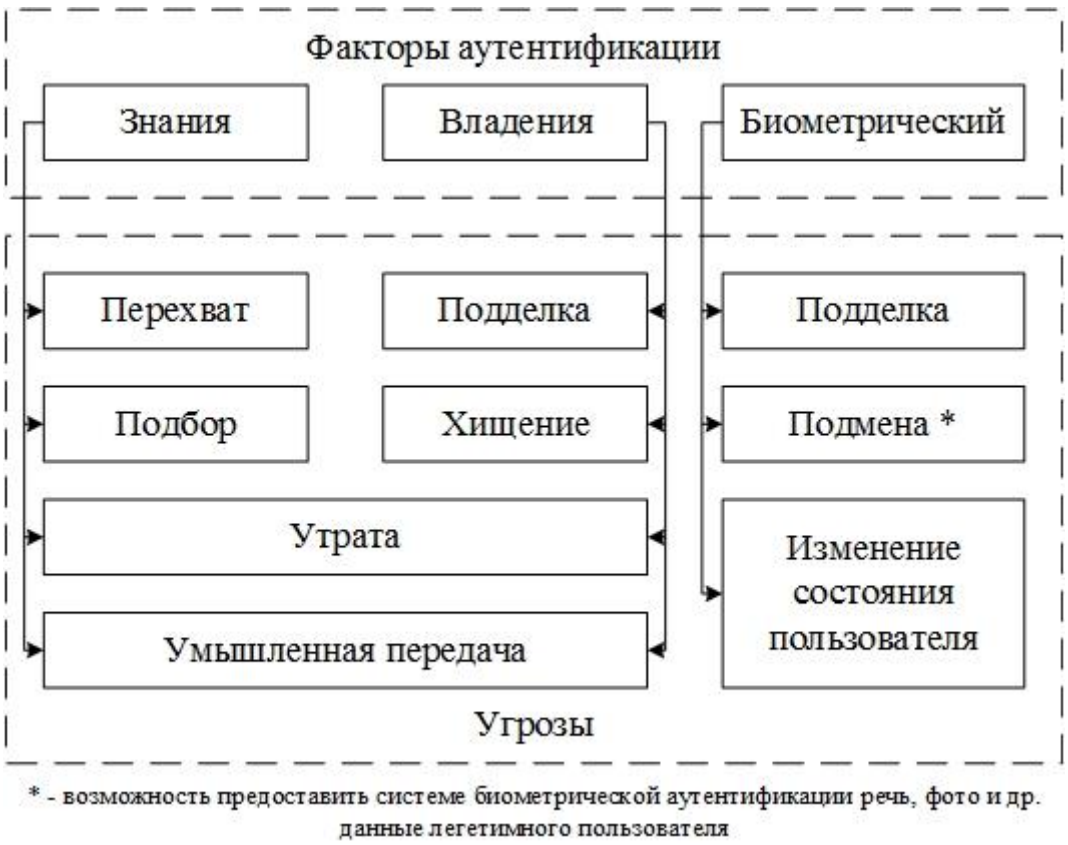

Рис. 2. Угрозы, которым подвержены существующие системы аутентификации
Fig. 2. Threats to Existing Authentication Systems

Кроме того, существующие системы выполняют процедуру аутентификации только при входе пользователя в систему, поэтому не выполняется требование к непрерывности аутентификации, которое характеризует способность контролировать истинность пользователя на протяжении всего сеанса работы. Данное свойство обусловлено наличием способов обхода классических средств разграничения доступа. Так, проведенные исследования показали, что около 85% негативного влияния осуществляется аутентифицированными пользователями, при этом по вине внутренних нарушителей до 64,5%, при этом в 53,5% случаев виновными в утечке информации оказались штатные сотрудники [9].

Обоснование необходимости применения многомодальной аутентификации пользователей

Для разграничения доступа к ресурсам критической информационной инфраструктуры целесообразно применять многомодальную аутентификацию. Методы многомодальной аутентификации позволяют учитывать информацию о функциональном состоянии пользователя, способствуя повышению достоверности процедуры [11, 12].

Многомодальное взаимодействие реализуется путем использования средств передачи информации по различным каналам [13] (рис. 3). При обработке потоков входной информации учитывается передаваемая пользователем семантическая информация, при этом способы ее ввода (модальности) можно разделить на активные (непосредственно речь, жесты) и пассивные (появление морщин, движение глаз и др.).

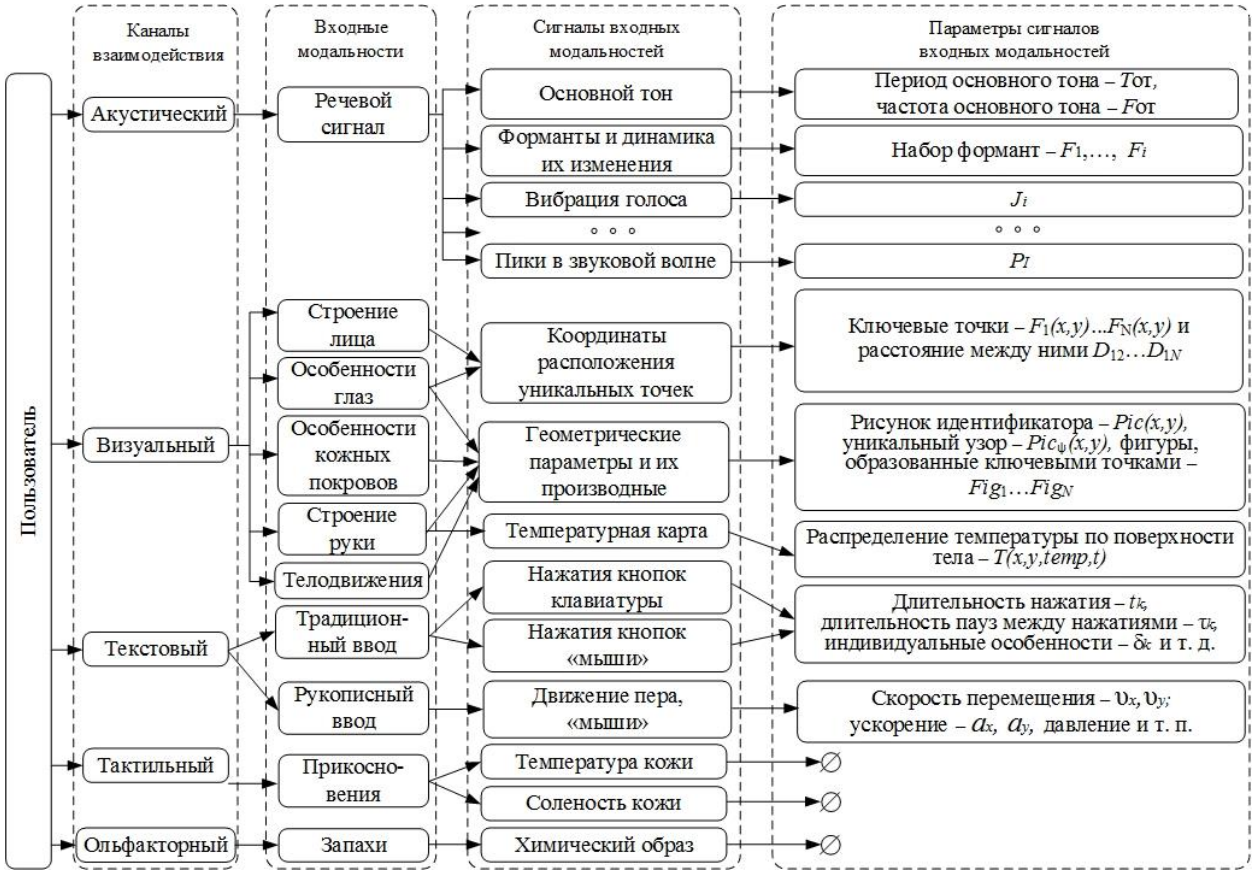

Рис. 3. Каналы взаимодействия пользователя с автоматизированной системой при проведении процедуры аутентификации

Fig. 3. User interaction channels with the automated system during the authentication procedure

В акустическом канале взаимодействия основной передаваемой информацией является речь пользователя. При аутентификации по голосу применяются методы определения частоты основного тона, коэффициентам линейного предсказания, перцепционным коэффициентам линейного предсказания, мел-кепстральным коэффициентам [15].

В текстовом канале взаимодействия осуществляется выделение биометрических признаков с помощью традиционного (клавиатура, мышь) и рукописного ввода. Сбор информации о работе пользователя реализуется путём непосредственного замера временных значений нажатий и отпускания клавиш, вычислении их различных комбинаций (интервалов между нажатием клавиш, интервалов времени удержания клавиш [16]), определения функций изменения координат, давление и угла наклона к плоскости при работе с пером [23], движения и нажатия кнопок мыши [17, 18].

В визуальном канале взаимодействия осуществляется выделение биометрических признаков лица [19] (координаты и расстояние между характерными точками, термограмма), глаз (рисунок кровеносных сосудов глазного дна), рук (форма, изгиб пальцев и т.д.).

В тактильном канале взаимодействия выделяются такие признаки, как температура и уровень солености кожи.

В ольфакторном канале взаимодействия выделяют признаки с помощью кожного покрова (запах тела), однако из-за сложности получения и обработки информации по данному каналу такие системы в настоящее время не получили распространения.

Таким образом, при обработке потоков информации в многомодальных системах учитывается семантическая информация, передаваемая пользователем. Учет девиации его биометрических параметров, вызванных изменением состояния, является одним из направлений повышения достоверности многомодальной аутентификации [14].

Анализ проведенных исследований показывает, что разные биометрические параметры вносят различный вклад в достоверность аутентификации (рис. 4).

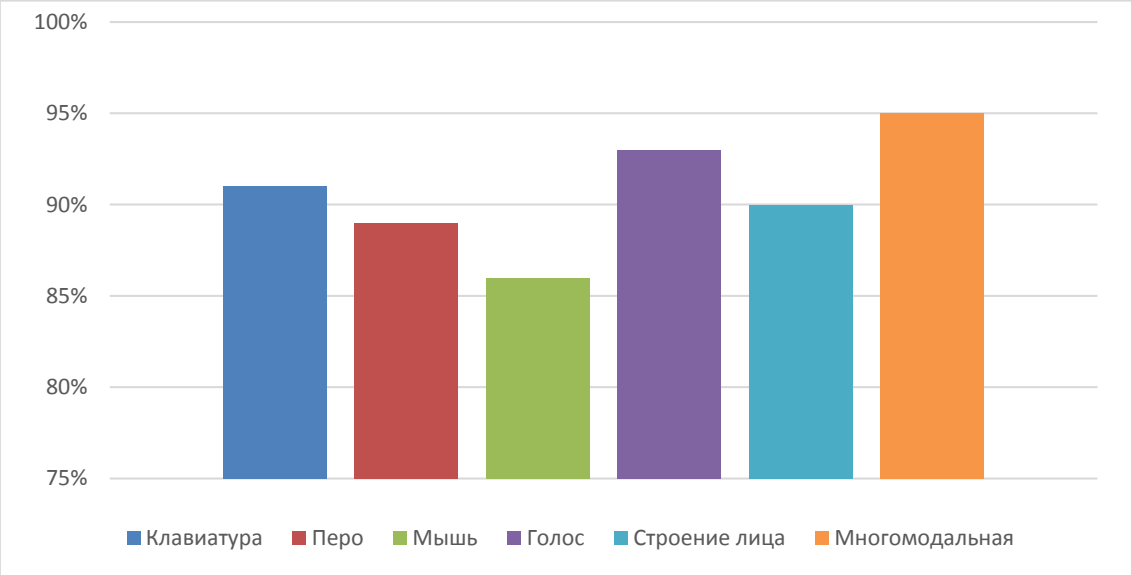

Рис. 4. Сравнение результатов моделирования системы многомодальной аутентификации с существующими решениями

Fig. 4. Comparison of the system simulation results multimodal authentication with existing solutions

Данные для различных каналов взаимодействия, полученные при моделировании [4] системы многомодальной аутентификации, согласуются с известными показателями [20-22]. При этом достоверность многомодальной аутентификации составила 95%, что превышает одномодальную на 2-6% в нормальных условиях (нормальном состоянии пользователя). При этом вероятность ошибок первого рода составила 0,81%, а вероятность ошибок второго рода 0,25%.

Таким образом, применение методов многомодальной аутентификации вносит существенный вклад в увеличение достоверности системы аутентификации.

ЗАКЛЮЧЕНИЕ

На сегодняшний день при использовании традиционных методов аутентификации объекты критической информационной инфраструктуры остаются подвержены угрозе несанкционированного доступа, обусловленной наличием ряда существенных недостатков в таких методах. Многомодальная аутентификация лишена недостатков классических методов, что в существенной степени повышает достоверность процедуры аутентификации и способствует снижению вероятности НСД к объектам КИИ.

Список литературы

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

2. Приказ ФСТЭК России № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (Зарегистрировано в Минюсте России 26.03.2018 № 50524).

3. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения.

4. Никитин В.В. Модель и методика многомодальной аутентификации пользователя автоматизированной системы: Автореф… дис. канд. техн. наук. – Воронеж 2018. – 18 с.

5. Бойченко О.В. Обеспечение безопасности критически важных объектов инфраструктуры Российской Федерации. / О.В. Бойченко, А.А. Аношкина А.А. // Ученые записки Крымского федерального университета имени В.И. Вернадского. Экономика и управление. Том 2. 2016 г. С. 15 – 19.

6. Мартынова Л.Е. Исследование и сравнительный анализ методов аутентификации / Л.Е. Мартынова, М.Ю. Умницын, К.Е. Назарова, И.П. Пересыпкин // Молодой ученый. – 2016. – № 19. С. 90-93.

7. ГОСТ Р 52633.0-2006 Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации

8. Никитин В.В. Существующие системы аутентификации и идентификации пользователей: основные проблемы и направления их модернизации // Вестник Московского Университета МВД России. – 2014. – № 2. – С. 165-172.

9. Отчёт об исследовании утечек конфиденциальной информации аналитического центра компании InfoWatch за 2018 г. – https:// www.infowatch.ru/sites/default/files/report/analytics/russ/infowatch_global_report_2018_half_year.pdf?rel=1, дата обращения 21.08.2019 г.

10. ГОСТ Р ИСО/МЭК 9594 – 8 – 98 – Ч. 8. Основы аутентификации.

11. Басов О.О. Карпов А.А., Саитов И А. Методологические основы синтеза полимодальных инфокоммуникационных систем государственного управления: монография. – Орёл: Академия ФСО России, 2015. – 270 с.

12. Болл Руд М. и др. Руководство по биометрии. – Москва: Техносфера, 2007. – 368 с.

13. Носов М.В., Басов О.О. Оценивание психофизиологического состояния человека по сигналам различных каналов взаимодействия с техническими средствами автоматизированных рабочих мест / Мат. 4-й Межд. научн.-практ. конф. «Современные инновации в науке и технике» (18.04.2014 г.) / Редкол.: Горохов А.А. (отв. ред); Юго-Зап. гос. ун-т. В 3-х томах, Том 2., Курск, 2014. – С.72–75.

14. Басов О.О., Никитин В.В. Подход к совершенствованию системы аутентификации пользователей автоматизированной системы / Информационные системы и технологии, 2018. – № 5 (109). – С. 99-107.

15. Кухарев Г.А. Биометрические системы: методы и средства идентификации личности человека. – Санкт-Петербург: Политехника, 2001 – 240 с.

16. Борисов Р.В. Многофакторная система аутентификации пользователей по динамическим биометрическим признакам / Р.В. Борисов, В.В. Борисов, Н.Н. Буслаев, А.Е. Сулавко // Наука и инновации в технических университетах: сб. мат. конф. – Санкт-Петербург: СПбГТУ, 2008. – С. 61-62.

17. Тушканов Е.В., Гатчин Ю.А., Сухостат В.В. Метод аутентификации при использовании клавиатурного почерка на основе психофизиологического состояния пользователя // «Вестник компьютерных и информационных технологий» – Москва, 2015. – № 8. – С. 29-34.

18. Никитин В.В., Басов О.О. Учет психофизиологического состояния пользователя при его аутентификации по рукописному почерку / Сб. научных трудов 4-ой Межд. н.-практ. конф. «Инновации, качество и сервис в технике и технологиях» / ред. колл. Горохов А.А. (отв. ред.), в 3-х томах. Том. 2. Юго-Зап. гос. ун-т, Курск, 2014. – С. 41-44.

19. Кузнецов Д.А. Классификация методов обнаружения и распознавания лица на изображении / Кузнецов Д.А., Никольский П.Г., Рачков Д.С., Кузнецов А.В., Хахамов А.П. // Научный результат. Информационные технологии. Т.4, №1, 2019.

20. Тушканов Е.В. Сухостат В.В. Методы и алгоритмы аутентификации при использовании клавиатурного почерка на основе психофизиологического состояния пользователя // III Междунар. научно-практ. конф.: сб. научных статей / Под. ред. С.М. Доценко, – Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2014 г. – С. 111-114.

21. Сулавко А.Е. Разработка технологии биометрической идентификации пользователей по динамике набора парольной фразы // Научная сессия: сб. мат. конф. / ТУСУР. – Томск, 2011. – Т. 3. – С. 278-280.

22. Комплексированная система идентификации личности по динамике подсознательных движений / Б.Н. Епифанцев, П.С. Ложников, А.Е. Сулавко, Р. В. Борисов // Безопасность информационных технологий. – 2011. – № 4. – С. 97-102.

23. Мураматсу, Д., Мацумото, Т., Эффективность перьевого давления, Азимут и функции высоты для проверки подписи в режиме онлайн. Материалы Международной конференции по достижениям в области биометрии (МКБ), лекции по информатике 4642, Спрингер, с. 503-512.

References

1. Federal law of 26.07.2017 No. 187-FL "About safety of critical information infrastructure of the Russian Federation".

2. Order of FSTEC of the Russian Federation No. 239 "On Approval of Requirements for Ensuring Security of Important Objects of Critical Information Infrastructure of the Russian Federation" (Registered in the Ministry of Justice of the Russian Federation 26.03.2018 № 50524)

3. GOST 34.003-90. Information technology. Set of standards for automated systems. Automated systems. Terms and definitions.

4. Nikitin V.V. Model and methodology of multimodal authentication of the user of the automated system: Autoref... dis. candidate of engineering sciences. – Voronezh 2018. – 18 p.

5. Boychenko O.V. Ensuring the security of critical infrastructure facilities of the Russian Federation / O.V. Boychenko, A.A. Anoshkin A.A.//Scientists notes of the Crimean Federal University named after V.I. Vernadsky. Economics and management. Volume 2. 2016. C. 15 – 19.

6. Martynova L.E. Research and comparative analysis of authentication methods / L.E. Martynova, M.J. Umnitsin, K.E. Nazarov, I.P. Perepkin // Young scientist. – 2016. – № 19. P 90 – 93.

7. GOST R 52633.0-2006 Data protection. Information protection technique. Requirements for highly reliable biometric authentication

8. Nikitin V.V. Existing systems of authentication and identification of users: main problems and directions of their modernization // Journal of the Moscow University of the Ministry of Internal Affairs of the Russian Federation. – 2014. – № 2. – P.165-172.

9. Report on the investigation of leaks of confidential information of InfoWatch analytical center for 2018 – https://www.infowatch.ru/sites/default/files/report/analytics/russ/infowatch_global_report_2018_half_year.pdf?rel=1, date of appeal 21.08.2019.

10. GOST R ISO/IEC 9594 – 8 – 98 – Part 8. Authentication basics.

11. Basov O.O. Karpov A.A., Saitov and A. Methodological bases of synthesis of polymodal infocommunication systems of public administration: monograph. – Eagle: Academy of FSO of Russia, 2015. – 270 p.

12. Ball Rud M. et al. Biometrics Manual. – Moscow: Technosphere, 2007. 368 p.

13. Nosov M.V., Basov O.O. Assessment of psychophysiological state of a person by signals of various channels of interaction with technical means of automated workplaces/Mat. 4th International Study – Report Cont. "Modern Innovations in Science and Technology" (18.04.2014) / Redkol.: Gorokhov A.A. (red); South-Zap. State. un-t. In 3 volumes, Vol. 2., Kursk, 2014. – C.72-75.

14. Basov O.O., Nikitin V.V. Approach to Improvement of User Authentication System of Automated System / Information Systems and Technologies, 2018. – № 5 (109). – P 99-107.

15. Kukharev G.A. Biometric Systems: Methods and Means of Identification of a Person. – St. Petersburg: Polytechnic, 2001 – 240 p.

16. Borisov R.V. Multi-factor system of authentication of users by dynamic biometric signs / R.V. Borisov, V.V. Borisov, N. N. Buslayev, A.E. Sulavko // Science and innovation in technical universities: mat. cont. – St. Petersburg: SPbGTU, 2008 – 61-62.

17. Tushkanov E.V., Gatchin Yu. A., Sukhostat V.V. Method of authentication when using keyboard handwriting based on the psychophysiological state of the user//"Journal of Computer and Information Technologies" – Moscow, 2015. – № 8. – P 29-34.

18. Nikitin V.V., Basov O.O. Taking into account the psychophysiological state of the user during his authentication by handwriting/SB of scientific works of the 4th International State Committee. "Innovation, Quality and Service in Technology and Technology"/ed. Call. Gorogov A.A. (ed.), in 3 volumes. Tom. 2. South-Zap. state. un-t, Kursk, 2014. – P.41-44.

19. Kuznetsov D.A. Classification of methods of detection and facial recognition on the image / Kuznetsov D.A., Nikolsky P.G., Rachkov D.S., Kuznetsov A.V., Khakhamov A.P. // Scientific result. Information technology. T.4, No. 1, 2019.